Chronique
Régulation et conformité

MARTINE BOCCARA
Conformité -
Protection des intérêts
Clients
BNP Paribas

EMMANUEL JOUFFIN
Docteur en droit
Responsable
juridique
de banque

MYRIAM ROUSSILLE
Agrégée
des facultés de droit
Professeur
Université du Mans
IRJS Sorbonne
Affaires-Finance

Projet de loi Informatique et Libertés II – Le bateau ivre

Commentaire d'Emmanuel Jouffin

Il n'est pas accoutumé de commenter dans ces colonnes un texte se trouvant à un stade embryonnaire de sa procédure législative et qui, de surcroît, fait un large renvoi à une ordonnance qui, schématiquement, devrait être le principal siège de la réforme annoncée. Toutefois, l'importance du sujet, et un calendrier de mise en œuvre du RGPD des plus contraint, nous conduisent à souligner quelques-uns des points saillants relatifs à la délicate œuvre de mise en conformité de leurs traitements qui attend, notamment, les établissements bancaires.

En guise de préambule, on ne peut que souligner l'opinion du Conseil d'État, lequel précise dans son avis : « *La technique mise en œuvre aboutit cependant à un résultat très insatisfaisant en termes de lisibilité du droit positif* ». Il poursuit en indiquant : « *Chaque fois que le Gouvernement souhaite utiliser l'une des 56 marges de manœuvre nationales ouvertes par le règlement, il s'efforce de réécrire les dispositions nécessaires, qu'elles soient plus exigeantes ou au contraire plus souples, plutôt que de répéter le principe posé par le règlement.* »

1. UN TEXTE QUI ANNONCE UNE RÉFORME…MAIS NE LA PORTE PAS

Quelques remarques générales sur ce projet. Tout d'abord, la mission assignée à cette réforme est double : d'une part, la transposition de la directive 2016/680 du 27 avril 2016[1] ; d'autre part, la mise en conformité du droit national au contenu du RGPD[2]. La particularité de ce règlement, lequel est en principe un acte juridique d'application *ne varietur* dans les États membres[3], est de comporter un nombre très substantiel de « *discrétions nationales* »[4], sur des sujets qui sont loin d'être ancillaires. Cette particularité fait douter, d'une part, de la réelle portée de l'uniformisation au niveau européen du droit en la matière et laisse augurer, d'autre part, d'ajustements ultérieurs sous des formes diverses et variées.

Ceci rappelé, on pouvait légitimement s'attendre à ce que le projet de loi éclaire la lanterne des responsables de traitements sur ces nombreuses discrétions nationales, leur permettant ainsi d'aborder plus sereinement la date du 25 mai 2018, date d'application du RGPD. Il n'en est rien.

Nous l'avons dit, une ordonnance ayant pour objet, notamment, de réécrire l'ensemble de la loi Informatique et Libertés première du nom (art. 20-I-1° du projet) devrait être le vecteur principal de la réforme, objectif que l'on aurait pu penser être celui du projet de loi lui-même. L'article 20 dudit projet prévoit en effet de confier au gouvernement, par voie d'ordonnance[5], non seulement la mission de réécrire l'ensemble de la loi « *afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence ainsi qu'à la simplicité de la mise en œuvre*

1. Directive relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Elle doit être transposée d'ici le 6 mai 2018.
2. Règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Ce texte sera applicable le 25 mai 2018.
3. Article 288 du traité sur le fonctionnement de l'Union européenne (TFUE) : le règlement revêt une portée générale et obligatoire, dans tous ses éléments, directement applicable dans tous les pays de l'Union européenne.
4. 56 selon le décompte opéré par le Secrétariat général aux affaires européennes.
5. Dans le délai de 6 mois à compter de la promulgation du projet de loi.

par les personnes concernées des dispositions qui mettent le droit national en conformité avec le RGPD », mais également le soin d'« *apporter les modifications qui seraient rendues nécessaires pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions résultant de la présente loi, et abroger les dispositions devenues sans objet* ». L'objectif est louable, la question est toutefois celle du délai d'adoption de ces mesures, question d'autant plus sensible que le projet de loi est muet sur des sujets clés tels que le profilage, les mentions d'information, ou bien encore la portabilité. Ce dernier sujet, abordé dans le Code de la consommation[6] suite à la loi Lemaire, aurait mérité d'être traité de manière unique dans le périmètre de la réforme de la loi de janvier 1978.

2. UN RENFORCEMENT SUBSTANTIEL DES POUVOIRS DE LA CNIL ET DE SON PRÉSIDENT (ARTICLE 1ER)

2.1. Extension du pouvoir réglementaire de la CNIL

Un des sujets les plus amplement traité par le projet de loi est le pouvoir normatif de la CNIL, notablement renforcé[7] par la possibilité qui lui est offerte de diffuser des lignes directrices, recommandations ou référentiels « *destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants* ». Par ailleurs, la CNIL se voit confier la mission d'« *encourage[r] l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables du traitement et aux sous-traitants* ».

S'y ajoute un autre « encouragement », cette fois-ci à « *l'élaboration de codes de conduites, établissement et publication de règlements types en vue d'assurer la sécurité des systèmes, pouvant contenir des prescriptions techniques et organisationnelles supplémentaires* ». On ignore quelles seront les formes de ces encouragements, qui devraient se porter, tant vers les responsables de traitements, que vers les organisations professionnelles représentatives. Par ailleurs, la normativité des « règlements types » dans le domaine de la sécurité se posera d'autant plus qu'il y a déjà, dans ce domaine, pléthore de textes[8].

On notera particulièrement le contenu de l'article 1-9° qui prévoit que la CNIL « *peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable* ». Le sujet est ici celui de la détermination du périmètre des analyses d'impacts, seuls vestiges (modulo les remarques que nous ferons ci-après) des autorisations préalables. Ces analyses sont nécessaires pour les traitements comportant des risques particuliers pour les personnes[9], la consultation de l'autorité de contrôle n'étant obligatoire qu'en présence d'un risque élevé qui ne peut-être atténué par des moyens raisonnables[10]. On notera que l'article 35-4 du RGPD fait de la réalisation et de la publication de ces listes, non pas une faculté comme l'indique le projet de loi, mais bien une obligation pour les autorités nationales de protection des données.

Avant longtemps, la CNIL sera sans doute amenée à produire sa politique de transparence explicitant auprès des responsables de traitement la portée de ses nouveaux pouvoirs réglementaires. Cette production viendra en sus de celle issue du Comité européen de la protection des données[11] qui, remplaçant le G29, aura lui aussi pour mission de publier des lignes directrices, recommandations et bonnes pratiques dans des domaines divers (art. 70 du RGPD). Ce Comité détiendra également le pouvoir d'émettre des avis contraignants (art. 70, paragraphe t, du RGPD). Par ailleurs, la CNIL se voit attribuer un rôle de conseil auprès des présidents de l'Assemblée nationale et du Sénat (art. 1 et 10° du projet de loi) en matière de protection des données, rôle qu'assume, au niveau des institutions européennes, le contrôleur européen à la protection des données[12].

Souhaitons l'absence de cacophonies entre ces divers acteurs, chargés de faire respecter une unicité de réglementation que le RGPD échoue à mettre en œuvre.

2.2. Un rôle d'*amicus curiae*

L'article premier 11° prévoit la possibilité pour la CNIL de présenter des observations devant « *toute juridiction* » au sujet de l'application du RGPD. Cette faculté s'étend sans doute aux observations présentées devant l'ACPR, la Commission des sanctions de cette dernière s'étant reconnu la qualité de juridiction au sens de l'article 267 du TFUE[13].

La CNIL rejoint ainsi la DGCCRF qui, en vertu de l'article L. 215-21 du Code de la consommation, peut également agir en tant qu'*amicus curiae* devant les juridictions civiles, pénales et l'Autorité de la concurrence, notamment en matière de clauses abusives[14]. La question est de savoir si ce statut d'*amicus curiae* accordé à la CNIL serait compatible avec celui de partie poursuivante devant une juridiction correctionnelle.

6. Article L. 224-42-3 du Code de la consommation.

7. Conformément aux articles 38 et suivants du RGPD.

8. Art 33 et 34 du RGPD, art. 4.4 et 4.7 de la directive 2016/1148 dite directive NIS, art. L. 521-10-I du CMF (issu de l'article 96 de la DSP 2), art. 10 ak de l'arrêté du 3 novembre 2014 sur le contrôle interne (modifié le 31 août 2017), Art. L. 1332-6-2 du Code de la défense : incidents affectant le fonctionnement ou la sécurité des systèmes d'information des opérateurs d'importance vitale (texte issu de Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019).

9. Art. 35 et 36 du RGPD : *Scoring*, données sensibles, vidéosurveillance, données génétiques ou biométriques, usage de nouvelles technologies…

10. Considérant 94 du RGPD.

11. Articles 68 à 76 du RGPD.

12. Création du Règlement n° 45/2001 du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

13. La Commission des sanctions de l'ACPR est une juridiction : décision ACPR n° 2010-06 *bis* du 13 mai 2011.

14. Article L. 141-1- IX du Code de la consommation. Ce texte doit être complété par un décret d'application.

2.3. Renforcement des pouvoirs d'enquête

L'article 4-3° du projet octroie à la CNIL des pouvoirs d'enquête renforcés. Tout d'abord, est énoncée une inopposabilité du « secret » sans plus de précision, ce qui concerne sans doute le secret bancaire et des affaires[15]. Le projet de loi reprend ici la faculté offerte aux États par l'article 90 du RGPD. Une harmonisation des règles au niveau européen est nécessaire.

Par ailleurs, la CNIL aura la possibilité, « *sur place ou sur documentation* », de « *demander communication de tous documents* » sur tous supports et en prendre copie. Pas un mot n'est dit sur l'indemnisation des frais de copie, ni évocation d'une quelconque proportionnalité dans les demandes de copie. Enfin, est prévu le recours à une identité d'emprunt. Le texte précisant que le recours à une telle identité « *est sans incidence sur la régularité des constatations effectuées* ». Un décret en Conseil d'État est attendu à ce sujet.

La CNIL aura ainsi les mêmes pouvoirs que la DFCCRF, dont les agents peuvent, eux aussi, recourir à une identité d'emprunt[16]. Enfin, on rappellera que cette même DGCCRF est également compétente pour contrôler et enquêter sur le respect de la loi informatique et libertés. Ainsi, l'article L. 511-9 du Code de la consommation permet à ses agents de constater les infractions et manquements aux chapitres II[17], IV[18]et V[19] de la loi n° 78-17 du 6 janvier 1978 et de communiquer ses constatations à la CNIL.

2.4. Renforcement des pouvoirs répressifs

On soulignera principalement que l'article 6 du projet de loi prévoit un pouvoir d'avertissement et de mise en demeure par le président de la CNIL (art. 45-I et 45-III) et de sanctions (art. 45-II), l'avertissement étant lié à un traitement « *susceptible de violer les dispositions* » du RGPD. Sans doute faut-il voir là une incitation forte au recours à une étude d'impact. Toutefois, la notion de « susceptibilité » est trop imprécise et ne peut raisonnablement servir de fondement à une sanction, fût-ce un avertissement.

Par ailleurs, le président de la CNIL peut saisir la formation restreinte en vue du prononcé de sanctions graduées allant du rappel à l'ordre à l'amende administrative d'un montant pouvant atteindre 4 % du chiffre d'affaires annuel consolidé en passant par une injonction de mise en conformité du traitement ou de réponse aux demandes présentées par une personne concernée. Cette injonction peut être assortie d'une astreinte dont le montant ne peut excéder 100 000 euros par jour.

On notera que le projet de loi tente de limiter le cumul de sanctions administratives et pénales. L'article 6-6° du projet de loi prévoit en effet que le juge pénal peut décider que, si une amende administrative intervient avant qu'il ait statué définitivement, ladite sanction peut être imputée sur le montant de l'amende pénale. Pour autant, cette mesure ne répond pas à la question de la nature pénale des sanctions prévues par le RGPD. En effet, compte tenu du montant des sanctions administratives qui peuvent être prononcées, on a le plus grand mal à admettre la qualification administrative de ces dernières. On notera que la Cour EDH, dans un arrêt remarqué du 10 février 2009[20], a requalifié en sanction pénale une sanction qualifiée d'administrative en droit national. Cette décision puise sa source dans un arrêt *Engel c/Pays-Bas*[21] énonçant clairement le caractère subsidiaire des qualifications des sanctions retenues par les États.

L'article 6-II-6° permettrait à la CNIL de décider du retrait de la décision d'approbation d'une règle d'entreprise contraignante (BCR). Une telle mesure devrait être entourée de garanties suffisantes au regard de l'investissement que représente le processus d'élaboration et d'adoption de ces règles.

Enfin, l'article 6-IV du projet de loi prévoit que la CNIL puisse ordonner à un responsable du traitement ou à un sous-traitant, à ses frais, une mesure d'information individuelle de chaque personne concernée par une violation d'une quelconque disposition de la loi Informatique et Libertés ou du RGPD. Cette disposition, ajout purement français, semble manquer de toute proportionnalité. La notification des alertes auprès des clients doit demeurer une mesure exceptionnelle. Sa généralisation risque de devenir contre-productive, conduisant à sa banalisation et donc à son inutilité.

3. LE RÉGIME DES FORMALITÉS AUPRÈS DE LA CNIL

Le RGPD a supprimé les formalités préalables auprès des autorités de contrôle au bénéfice d'un principe d'*accountability*[22], exception faite de la consultation préalable de la CNIL en cas de traitement présentant un risque après l'analyse d'impact sur les données personnelles ou des mesures de sauvegarde pour les transferts. Toutefois, le projet de texte est ambigu sur ce sujet. Il maintient des formalités préalables pour les données de santé (art. 13), mais aussi (art. 9) pour les traitements impliquant l'usage du NIR.

15. Exception faite du secret des avocats, des sources journalistiques et du secret médical.
16. Article L.512-16 du Code de la consommation.
17. Conditions de licéité des traitements de données à caractère personnel.
18. Formalités préalables à la mise en oeuvre des traitements, prérogatives qui devrait essentiellement s'appliquer aux études d'impact sur la vie privée.
19. Obligations incombant aux responsables de traitements et droits des personnes.
20. Arrêts CEDH 10 février 2009, *Zolotoukhine c/ Russie* ; CEDH 25 juin 2009, *Maresti c/ Croatie* ; CEDH 16 juin 2009, *Ruotsalainen c/ Finlande*.
21. CEDH 8 juin 1976. La Cour EDH a ensuite rappelé à de nombreuses reprises qu'elle n'était pas liée par les qualifications retenues en droit interne : CEDH 21 février 1984, *Öztürk c/ Allemagne*, § 49-50 ; CEDH 9 février 1995, *Welch c/ Royaume-Uni*, § 27, série A, n° 307-A ; *Jamil c/ France*, 8 juin 1995, § 30, série A, n° 317-B ; CEDH 23 septembre 1998 ; *Malige c/ France*, § 34 ; CEDH 28 octobre 1999, *Escoubet c/ Belgique*, § 35.
22. Articles 5-2 et 24.

À cet égard, si l'article 9 du projet abroge les articles 24 et 25 de la loi Informatique et Libertés, il ne supprime pas l'article 23 relatif aux déclarations des traitements, disposition obsolète. Le projet de loi manque de cohérence sur ce sujet sensible des formalités préalables. Ainsi, on soulignera le maintien de la référence aux autorisations pour les transferts hors UE dans l'article 6, dernier paragraphe, de la loi Informatique et libertés, ce dernier n'ayant fait l'objet d'aucune modification par le projet de loi. Cette question sera peut-être abordée par l'ordonnance visée à l'article 20 du projet.

S'agissant du sort réservé aux autorisations obtenues sous l'empire de la loi Informatique et Libertés I, le sujet n'est, à ce jour, pas abordé par le projet de loi. À ce sujet, on fera les remarques suivantes. Tout d'abord, le considérant 171 du RGPD prévoit que « *les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées* ». Le G29, sans grande surprise, reprend la philosophie de l'*accountability*[23] dans ses lignes directrices relatives à l'EIVP[24] et précise : « *À titre de bonne pratique, une DPIA devrait être effectué en permanence sur les activités de traitement existantes. Cependant, il devrait être réévalué après 3 ans, peut-être plus tôt, selon la nature du traitement et le taux de changement dans le traitement et les circonstances générales. Une telle évaluation est également recommandée pour le traitement des données ayant eu lieu avant mai 2018 et donc non soumis à une DPIA, pour s'assurer que 3 ans après cette date ou plus tôt, selon le contexte, les risques pour les droits et libertés sont encore atténué* »[25].

4. TRANSFERTS DE DONNÉES HORS UE

L'article 17 du projet de loi donne la possibilité à la CNIL de saisir le Conseil d'État en vue d'ordonner la suspension ou la cessation d'un transfert de données, éventuellement sous astreinte, et assortir ses conclusions d'une demande de question préjudicielle à la CJUE[26]. Il va sans dire que, dans le contexte des recours déposés contre le *privacy shield*[27], cette faculté peut être particulièrement lourde de conséquences et devrait, à ce titre, faire l'objet de garanties préalables à la saisine du Conseil d'État, de telle sorte que soit évitée toute forme d'arbitraire à ce sujet.

5. TRANSPARENCE ALGORITHMIQUE (POUR LES DÉCISIONS ADMINISTRATIVES)

L'article 14 évoque en termes sibyllins, et sur un périmètre réduit, un principe de transparence algorithmique le responsable de traitement devant s'assurer « *[…] de la maîtrise du traitement algorithmique et de ses évolutions* » sans que l'on sache ce qu'est cette maîtrise[28]. Sur un sujet aussi complexe qu'important, on regrettera que le législateur ne prenne pas parti sur une transparence déjà présente dans le Code de la consommation[29].

Ce texte devrait être une opportunité pour lutter contre l'inquiétude que suscitent des algorithmes risquant d'enfermer les internautes dans un « *déterministe numérique* » conduisant à ce qu'une personne se réduise à la somme du traitement algorithmique des informations la concernant[30].

Une réflexion de fond sur les algorithmes devrait également conduire à s'interroger sur les données qui les alimentent et qui permettent d'identifier indirectement une personne. À ce jour, la CNIL et le Conseil d'État[31] ont une lecture rigoriste de l'article 2 de la loi Informatique et Libertés[32] qui aborde la question des données indirectement personnelles. À cet égard, afin de déterminer si une donnée est personnelle, il faut prendre en considération l'ensemble des moyens envisageables dont dispose ou auxquels peut avoir accès le responsable de traitement ou « *toute autre personne* » en vue de permettre une identification.

En clair, la qualification de données personnelles peut être retenue, même si l'identification de la personne concernée est rendue très difficile, voire improbable et nécessite pour cela le recours à des moyens considérables. Pratiquement, toute donnée déversée dans un *data lake* peut, pour peu que l'on s'en donne les moyens, être algorithmiquement associée à d'autres, permettant ainsi une identification indirecte. Ce sujet est lourd de conséquences s'agissant du *Big Data*, lequel nécessite le traitement de données en gros volumes.

23. Articles 5-2 et 24 du RGPD.

24. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679, 4 avril 2017, spéc. p. 12

25. Traduction libre de « *As a matter of good practice, a DPIA should be continuously carried out on existing processing activities. However, it should be re-assessed after 3 years, perhaps sooner, depending on the nature of the processing and the rate of change in the processing operation and general circumstances. Such assessment is also recommended for data processing which have taken place before May 2018 and where therefore not subject to a DPIA, to make sure that 3 years after this date or sooner, depending on the context, the risks for the rights and freedoms are still mitigated.* »

26. Ceci constitue une réécriture substantielle de l'article 58-2 j du RGPD lequel prévoit que l'autorité de contrôle peut « *ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale* ».

27. Recours en annulation sur le fondement de l'article 263 du TFUE formé contre la décision d'exécution 2016/1250 du 12 juillet 2016 relative au *privacy shield* formé le 16 septembre 2016 par l'organisation de défense irlandaise Digital rights rejointe dans le cadre d'un second recours par la Quadrature du net, la French Data Network et la Fédération FDN.

28. S'agissant des obligations de transparence s'imposant d'ores et déjà à l'administration : art L. 300-2, L. 311-3-1 et R. 311-3-1-2 du Code des relations entre le public et l'administration.

29. Pour les plates-formes en ligne, v. art. L. 111-7-II-1° et D. 111-7-I du Code de la consommation et D. 111-15-I : Adoption de bonnes pratiques pour renforcer la loyauté, la clarté et la transparence des informations transmises aux consommateurs.

30. 57 % des Français pensent que les algorithmes limitent l'étendue des choix proposés, 64 % considèrent que les algorithmes représentent plutôt une menace en raison de l'accumulation des données personnelles détenues (source : Sondage IFOP pour la CNIL, janvier 2017).

31. Délib. n° 2015-255 du 16 juillet 2015, *Jean-Claude Decaux*, et arrêt du Conseil d'État du 8 février 2017.

32. « *Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.* »

À cet égard, le considérant 26 du RGPD nous invite à faire preuve de bon sens[33] et à prendre en considération les moyens « *raisonnablement susceptibles* » d'être mis en œuvre pour identifier des personnes à partir de données non personnelles. La loi Informatique et Libertés II devrait ainsi reprendre les termes de ce considérant à l'occasion d'une réécriture de l'article alinéa 2 de la loi de 1978. À ce sujet, le G29 lui-même est favorable à cette approche proportionnée, tenant compte de « *l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre* ». S'agissant des documents administratifs, la Commission d'accès aux documents administratifs (CADA), dans un avis de novembre 2015, estimait à cet égard que la prohibition de publier toute donnée à caractère personnel était excessive s'agissant de données n'intéressant, ni la vie privée ni la réputation des personnes concernées.

6. RELATIONS AVEC LES SOUS-TRAITANTS

Le projet de loi (art. 10) effectue un renvoi sibyllin au chapitre IV du RGPD[34], sans plus de précision. Eu égard, notamment, à la possible responsabilité conjointe entre le responsable du traitement et le sous-traitant (art. 26) et au risque de requalification (art. 28-10 du RGPD) si un sous-traitant venait à déterminer, *in fine*, les finalités et les moyens du traitement, un minimum de développements aurait été le bienvenu. À moins qu'il n'eût été préférable de ne rien dire et de s'en tenir à la lettre du RGPD.

7. *QUID* DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES ?

Ce dernier est l'un des grands absents du texte. Son rôle de « *chef d'orchestre* » de la protection des données à caractère personnel aurait sans doute mérité une précision s'agissant de son « *indépendance* ». À quel risque s'expose-t-il en exprimant son désaccord avec telle ou telle décision d'entreprise ? Certes le RGPD énonce une interdiction de relever de ses fonctions ou de pénaliser le DPD « *pour l'exercice de ses missions* »[35], mais au-delà de la mise en garde, quelle place pour un devoir d'alerte de la CNIL par le DPO ? L'article 39-d et e du RGPD prévoit simplement que délégué à la protection des données coopère avec l'autorité de contrôle et sert de point de contact. Cette « coopération » irait-elle jusqu'à l'alerte éthique en cas de désaccord du DPD avec sa hiérarchie, qui est supposée être la plus élevée de l'entreprise (art. 38-3 du RGPD) ?

ET PENDANT CE TEMPS…

Tandis que ce projet de loi est débattu, l'agitation autour de la protection des données personnelles se poursuit. Tout d'abord, l'Assemblée nationale a adopté, le 4 janvier 2018, une résolution européenne sur le marché unique du numérique[36], faisant suite au rapport d'information présenté le 6 décembre 2017[37].

Dans cette résolution, sont notamment évoquées :

– la question d'une harmonisation maximale avec nos partenaires européens pour l'adaptation de la législation française au RGPD ; une tâche ardue, au vu du nombre de discrétions autorisées par ce dernier ;

– celle de la création d'un droit à la portabilité des données non personnelles, alors même que le RGPD ne vise que la portabilité des données personnelles[38]. Ce droit devrait être assorti de limites strictes et ne porter atteinte, ni à la confidentialité des informations des entreprises, ni aux secrets commerciaux, tout en tenant compte des contraintes techniques. Par ailleurs, la détention d'informations afin de satisfaire à des obligations légales (on pense aux obligations de connaissance de la clientèle) devrait également faire l'objet d'une réflexion particulière relative au périmètre de cette portabilité.

Enfin, la proposition de règlement e-privacy est toujours en cours de discussion devant le Conseil de l'Union européenne, après qu'un texte a été adopté au Parlement. Ce règlement a pour objet d'une part, de remplacer la directive Vie privée 2002/58 et, d'autre part, de compléter le RGPD. Entre autres sujets sensibles, ce texte aborde des questions telles que les métadonnées, les *cookies* et, notamment, le rôle central du navigateur dans la collecte du consentement à la collecte d'informations. Le risque est celui d'une concentration des pouvoirs au niveau des navigateurs et donc des grands acteurs du net. Ce texte devait entrer en application le 25 mai 2018. Ce ne sera vraisemblablement pas le cas.

Puisque nous sommes en janvier, période traditionnelle des vœux, souhaitons que le législateur français fasse preuve de bon sens, le législateur européen de diligence et de pragmatisme et enfin la CNIL de bienveillance à l'égard de responsables de traitements à qui, décidément, rien n'est épargné. ■

33. « *Pour déterminer si une personne physique est identifiable [...] prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement* [...]. »

34. Responsable du traitement et sous-traitant.

35. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions (art. 38-3 du RGPD).

36. JORF n° 2 du 4 janvier 2018, texte n° 62.

37. http://www2.assemblee-nationale.fr/documents/notice/15/europe/rap-info/i0479/(index)/rapports-information.

38. Il s'agirait là d'une généralisation de l'article L. 224-42-3 du Code de la consommation, lequel énonce, sous réserve des textes relatifs au secret en matière de propriété intellectuelle (le secret bancaire n'est pas visé), que tout « *fournisseur d'un service de communication au public en ligne* » doit proposer gratuitement une fonctionnalité permettant la récupération « *par une requête unique, l'ensemble des fichiers ou données concernés* ».